COMPUTER SECURITY FUNDAMENTALS

THIRD EDITION

CHUCK EASTTOM

Computer Security Fundamentals

Third Edition

Chuck Easttom

PEARSON

800 East 96th Street, Indianapolis, Indiana 46240 USA

Computer Security Fundamentals, Third Edition

ISBN-13: 978-0-7897-5746-3
ISBN-10: 0-7897-5746-X

Library of Congress control number: 2016940227

Printed in the United States of America

First Printing: May 2016

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Executive Editor
Brett Bartow

Acquisitions Editor
Betsy Brown

Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Gill Editorial Services

Indexer
Brad Herriman

Proofreader
Paula Lowell

Technical Editor
Dr. Louay Karadsheh

Publishing Coordinator
Vanessa Evans

Cover Designer
Chuti Prasertsith

Compositor
Mary Sudul

Contents at a Glance

Table of Contents

Chapter 8: Encryption 184

About the Author

Chuck Easttom is a computer security and forensics expert. He has authored 20 books, including several on computer security, forensics, and cryptography. He holds 6 patents and 40 computer certifications, including many security and forensics certifications. He has conducted training for law enforcement, federal agencies, and friendly foreign governments. He frequently works as an expert witness in computer-related cases. He is also a frequent speaker on computer security topics at a variety of security-related conferences. You can visit his website at www.chuckeasttom.com.

About the Technical Reviewer

Dr. Louay Karadsheh has a Doctorate of Management in information technology from Lawrence Technological University, Southfield, Michigan. His research interest includes cloud computing, information assurance, knowledge management, and risk management. Dr. Karadsheh has published 11 articles in refereed journals and international conference proceedings and has extensive knowledge in operating system, networking, and security. Dr. Karadsheh has provided technical edits/reviews for several major publishing companies, including Pearson and Cengage Learning. He holds CISSP, CEH, CASP, CCSK, CCE, Security+, VCA-C, VCA-DCV, SCNP, Network+, and Mobility+ certifications.

Dedication

This book is dedicated to my wife, Teresa,
who has helped me become who I am.

Acknowledgments

The creation of a book is not a simple process and requires the talents and dedication from many people to make it happen. With this in mind, I would like to thank the folks at Pearson for their commitment to this project.

Specifically, I would like to say thanks to Betsy Brown for overseeing the project and keeping things moving.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Register your copy of *Computer Security Fundamentals* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780789757463 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

It has been more than 10 years since the publication of the original edition of this book. A great deal has happened in the world of computer security since that time. This edition is updated to include newer information, updated issues, and revised content.

The real question is: Who is this book for? This book is a guide for any computer-savvy person. That means system administrators who are not security experts or anyone who has a working knowledge of computers and wishes to know more about cyber crime and terrorism could find this book useful. However, the core audience will be students who wish to take a first course in security but may not have a thorough background in computer networks. The book is in textbook format, making it ideal for introductory computer security courses that have no specific prerequisites. That lack of prerequisites means that people outside the normal computer science and computer information systems departments could also avail themselves of a course based on this book. This might be of particular interest to law enforcement officers, criminal justice majors, and even business majors with an interest in computer security.

As was previously mentioned, this book is intended as an introductory computer security book. In addition to the numerous end notes, the appendixes will guide you to a plethora of additional resources. There are also review questions and practice exercises with every chapter. Appendix C contains the answers to the multiple choice questions for your review. Exercises and projects don’t have a single answer. They are intended to encourage the reader to explore, so answers will vary.

This book is not a cookbook for hackers. You will see exactly how hackers target a system and get information about it. You will also see step-by-step instructions on how to use some password-cracking utilities and some network-scanning utilities. You will also be given a reasonably in-depth explanation of various hacking attacks. However, you won’t see a specific step-by-step recipe for executing an attack.

This book assumes that you are a competent computer user. That means you have used a computer at work and at home, are comfortable with email and web browsers, and know what words like RAM and USB mean. For instructors considering this as a textbook, that means students will have had some basic understanding of PCs but need not have had formal computer courses. For this reason, there is a chapter on basic networking concepts to get you up to speed. For readers with more knowledge, such as system administrators, you will find some chapters of more use to you than others. Feel free to simply skim any chapter that you feel is too elementary for you.

Chapter 1

Introduction to Computer Security

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Identify the top threats to a network: security breaches, denial of service attacks, and malware
- Assess the likelihood of an attack on your network
- Define key terms such as *cracker*, *penetration tester*, *firewall*, and *authentication*
- Compare and contrast perimeter and layered approaches to network security
- Use online resources to secure your network

Introduction

Since the first edition of this book, the prevalence of online transactions has increased dramatically. In 2004 we had e-commerce via websites; in 2016 we have smart phone apps, the Internet of Things, as well as an expanded use of e-commerce websites. Internet traffic is far more than just humorous YouTube videos or Facebook updates about our vacations. Now it is the heart and soul of commerce, both domestic and international. Internet communication even plays a central role in military operations and diplomatic relations. In addition to smart phones, we now have smart watches and even vehicles that have Wi-Fi hotspots and smart technology. Our lives are inextricably intertwined with the online world. We file our taxes online, shop for a home online, book our next vacation online, and even look for a date online.

Because so much of our business is transacted online, a great deal of personal information is stored in computers. Medical records, tax records, school records, and more are all stored in computer databases. This leads to some very important questions:

1. How is information safeguarded?
2. What are the vulnerabilities to these systems?
3. What steps are taken to ensure that these systems and data are safe?
4. Who can access my information?

FYI: Where Is the Internet Going?

Obviously the Internet has expanded, as previously mentioned. We now have smart phones, smart watches, even smart cars. We have the Internet of things (IoT) which involves devices communicating on the Internet. What do you think the next 10 years will bring?

Unfortunately, not only has technology and Internet access expanded since the original publication of this book, but so have the dangers. How serious is the problem? According to a 2014 article in *SC Magazine*,[1] "Cyber-crime and economic espionage cost the global economy more than $445 billion annually, which a report from the Center for Strategic and International Studies, says puts cyber-crime on par with the economic impact of global drug trafficking."

Another study[2] looked at specific companies and the cost of cybercrime in 2013. That study reported, "We found that the average annualized cost of cyber-crime for 60 organizations in our study is $11.6 million per year, with a range of $1.3 million to $58 million. In 2012, the average annualized cost was $8.9 million. This represents an increase in cost of 26 percent or $2.6 million from the results of our cyber cost study published last year."

The situation is not improving, either. According to a Pricewaterhouse Coopers study, in 2015 38% more security incidents were detected than in 2014. The same study showed a 56% increase in theft of intellectual property.

In spite of daily horror stories, however, many people (including some law enforcement professionals and trained computer professionals) lack an adequate understanding about the reality of these threats. Clearly the media will focus attention on the most dramatic computer security breaches, not necessarily giving an accurate picture of the most plausible threat scenarios. It is not uncommon to encounter the occasional system administrator whose knowledge of computer security is inadequate.

This chapter outlines current dangers, describes the most common types of attacks on your personal computer and network, teaches you how to speak the lingo of both hackers and security professionals, and outlines the broad strokes of what it takes to secure your computer and your network.

In this book, you will learn how to secure both individual computers and entire networks. You will also find out how to secure data transmission, and you will complete an exercise to find out about your region's laws regarding computer security. Perhaps the most crucial discussion in this chapter is what

[1] http://www.scmagazine.com/cyber-crime-costs-445-billion-globally-gdps-take-hit/article/354844/

[2] http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

attacks are commonly attempted and how they are perpetrated. In this first chapter we set the stage for the rest of the book by outlining what exactly the dangers are and introducing you to the terminology used by both network security professionals and hackers. All of these topics are explored more fully in subsequent chapters.

How Seriously Should You Take Threats to Network Security?

The first step in understanding computer and network security is to formulate a realistic assessment of the threats to those systems. You will need a clear picture of the dangers in order to adequately prepare a defense. There seem to be two extreme attitudes regarding computer security. The first group assumes there is no real threat. Subscribers to this belief feel that there is little real danger to computer systems and that much of the negative news is simply unwarranted panic. They often believe taking only minimal security precautions should ensure the safety of their systems. The prevailing sentiment is, if our organization has not been attacked so far, we must be secure. If decision makers subscribe to this point of view, they tend to push a reactive approach to security. They will wait to address security issues until an incident occurs—the proverbial "closing the barn door after the horse has already gotten out." If you are fortunate, the incident will have only minor impact on your organization and will serve as a much-needed wakeup call. If you are unfortunate, then your organization may face serious and possible catastrophic consequences. One major goal of this book is to encourage a proactive approach to security.

People who subscribe to the opposite viewpoint overestimate the dangers. They tend to assume that talented, numerous hackers are an imminent threat to their system. They may believe that any teenager with a laptop can traverse highly secure systems at will. Such a worldview makes excellent movie plots, but it is simply unrealistic. The reality is that many people who call themselves hackers are less knowledgeable than they think they are. These people have a low probability of being able to compromise any system that has implemented even moderate security precautions.

This does not mean that skillful hackers do not exist, of course. However, they must balance the costs (financial, time) against the rewards (ideological, monetary). "Good" hackers tend to target systems that yield the highest rewards. If a hacker doesn't perceive your system as beneficial to these goals, he is less likely to expend the resources to compromise your system. It is also important to understand that real intrusions into a network take time and effort. Hacking is not the dramatic process you see in movies. I often teach courses in hacking and penetration testing, and students are usually surprised to find that the process is actually a bit tedious and requires patience.

Both extremes of attitudes regarding the dangers to computer systems are inaccurate. It is certainly true that there are people who have the understanding of computer systems and the skills to compromise the security of many, if not most, systems. A number of people who call themselves hackers, though, are not as skilled as they claim to be. They have ascertained a few buzzwords from the Internet and may be convinced of their own digital supremacy, but they are not able to effect any real compromises to even a moderately secure system.

The truly talented hacker is no more common than the truly talented concert pianist. Consider how many people take piano lessons at some point in their lives. Now consider how many of those ever truly become virtuosos. The same is true of computer hackers. Keep in mind that even those who do possess the requisite skills need to be motivated to expend the time and effort to compromise your system.

A better way to assess the threat level to your system is to weigh the attractiveness of your system to potential intruders against the security measures in place.

Keep in mind, too, that the greatest external threat to any system is not hackers, but malware and denial of service (DoS) attacks. Malware includes viruses, worms, Trojan horses, and logic bombs. And beyond the external attacks, there is the issue of internal problems due to malfeasance or simple ignorance.

Security audits always begin with a risk assessment, and that is what we are describing here. First you need to identify your assets. Clearly, the actual computers, routers, switches and other devices that make up your network are assets. But it is more likely that your most important assets lie in the information on your network. Identifying assets begins with evaluating the information your network stores and its value. Does your network contain personal information for bank accounts? Perhaps medical information, health care records? In other cases your network might contain intellectual property, trade secrets, or even classified data.

Once you have identified the assets, you need to take inventory of the threats to your assets. Certainly any threat is possible, but some are more likely than others. This is very much like what one does when selecting home insurance. If you live in a flood plain, then flood insurance is critical. If you live at a high altitude in a desert, it may be less critical. We do the same thing with our data. If you are working for a defense contractor, then foreign state-sponsored hackers are a significant threat. However, if you are the network administrator for a school district, then your greatest threat involves juveniles attempting to breach the network. It is always important to realize what the threats are for your network.

Now that you have identified your assets and inventoried the threats, you need to find out what vulnerabilities your system has. Every system has vulnerabilities. Identifying your network's specific vulnerabilities is a major part of risk assessment.

The knowledge of your assets, threats, and vulnerabilities will give you the information needed to decide what security measures are appropriate for your network. You will always have budget constraints, so you will need to make wise decisions on selecting security controls. Using good risk assessment is how you make wise security decisions.

Note

There are a number of industry certifications that emphasize risk assessment. The Certified Information System's Security Professional (CISSP) puts significant emphasis on this issue. The Certified Information Systems Auditor (CISA) places even more focus on risk assessment. One or more appropriate industry certifications can enhance your skillset and make you more marketable as a security professional. There are many other certifications including the CompTIA Certified Advanced Security Practitioner (CASP) and Security+ certifications.

Identifying Types of Threats

As was discussed in the last section, identifying your threats is a key part of risk assessment. Some threats are common to all networks; others are more likely with specific types of networks. Various sources have divided threats into different categories based on specific criteria. In this section we will examine threats that have been divided into categories based on the nature of the attack. Since the last edition of this book I have separated out one of the security breach subcategories into its own category: insider threats. Most attacks can be categorized as one of seven broad classes:

- **Malware:** This is a generic term for software that has a malicious purpose. It includes virus attacks, worms, adware, Trojan horses, and spyware. This is the most prevalent danger to your system.
- **Security breaches:** This group of attacks includes any attempt to gain unauthorized access to your system. This includes cracking passwords, elevating privileges, breaking into a server…all the things you probably associate with the term *hacking*.
- **DoS attacks:** These are designed to prevent legitimate access to your system. And, as you will see in later chapters, this includes distributed denial of service (DDoS).
- **Web attacks:** This is any attack that attempts to breach your website. Two of the most common such attacks are SQL injection and cross-site scripting.
- **Session hijacking:** These attacks are rather advanced and involve an attacker attempting to take over a session.
- **Insider threats:** These are breaches based on someone who has access to your network misusing his access to steal data or compromise security.
- **DNS poisoning:** This type of attack seeks to compromise a DNS server so that users can be redirected to malicious websites, including phishing websites.

There are other attacks, such as social engineering. The forgoing list is just an attempt to provide a broad categorization of attack types. This section offers a broad description of each type of attack. Later chapters go into greater detail with each specific attack, how it is accomplished, and how to avoid it.

Malware

Malware is a generic term for software that has a malicious purpose. This section discusses four types of malware: viruses, Trojan horses, spyware, and logic bombs. Trojan horses and viruses are the most widely encountered. One could also include rootkits, but these usually spread as viruses and are regarded as simply a specific type of virus.

According to Symantec (makers of Norton antivirus and other software products), a *virus* is "a small program that replicates and hides itself inside other programs, usually without your knowledge"

(Symantec, 2003). While this definition is a bit old, it still applies. The key characteristic of a computer virus is that it self-replicates. A computer virus is similar to a biological virus; both are designed to replicate and spread. The most common method for spreading a virus is using the victim's email account to spread the virus to everyone in his address book. Some viruses don't actually harm the system itself, but *all* of them cause network slowdowns due to the heavy network traffic caused by the virus replication.

The *Trojan horse* gets its name from an ancient tale. The city of Troy was besieged for an extended period of time. The attackers could not gain entrance, so they constructed a huge wooden horse and one night left it in front of the gates of Troy. The next morning the residents of Troy saw the horse and assumed it to be a gift, so they rolled the wooden horse into the city. Unbeknownst to them, several soldiers where hidden inside the horse. That evening the soldiers left the horse, opened the city gates, and let their fellow attackers into the city. An electronic Trojan horse works the same way, appearing to be benign software but secretly downloading a virus or some other type of malware onto your computer from within.

Another category of malware currently on the rise is *spyware*. Spyware is simply software that literally spies on what you do on your computer. Spyware can be as simple as a *cookie*—a text file that your browser creates and stores on your hard drive—that a website you have visited downloads to your machine and uses to recognize you when you return to the site. However, that flat file can then be read by the website or by other websites. Any data that the file saves can be retrieved by any website, so your entire Internet browsing history can be tracked. Spyware may also consist of software that takes periodic screenshots of the activity on your computer and sends those to the attacker.

Another form of spyware, called a *key logger*, records all of your keystrokes. Some key loggers also take periodic screenshots of your computer. Data is then either stored for later retrieval by the person who installed the key logger or is sent immediately back via email. We will discuss specific types of key loggers later in this book.

A *logic bomb* is software that lays dormant until some specific condition is met. That condition is usually a date and time. When the condition is met, the software does some malicious act such as delete files, alter system configuration, or perhaps release a virus. In Chapter 5, "Malware," we will examine logic bombs and other types of malware in detail.

Compromising System Security

Next we will look at attacks that breach your system's security. This activity is what is commonly referred to as *hacking*, though that is not the term hackers themselves use. We will delve into appropriate terminology in just a few pages; however, it should be noted at this point that *cracking* is the appropriate word for intruding into a system without permission, usually with malevolent intent. Any attack that is designed to breach your security, either via some operating system flaw or any other means, can be classified as cracking.

Essentially any technique to bypass security, crack passwords, breach Wi-Fi, or in any way actually gain access to the target network fits into this category. That makes this a very broad category indeed.

However, not all breaches involve technical exploits. In fact, some of the most successful breaches are entirely nontechnical. *Social engineering* is a technique for breaching a system's security by exploiting human nature rather than technology. This was the path that the famous hacker Kevin Mitnick most often used. Social engineering uses standard con techniques to get users to give up the information needed to gain access to a target system. The way this method works is rather simple: The perpetrator gets preliminary information about a target organization and leverages it to obtain additional information from the system's users.

Following is an example of social engineering in action. Armed with the name of a system administrator, you might call someone in the business's accounting department and claim to be one of the company's technical support personnel. Mentioning the system administrator's name would help validate that claim, allowing you to ask questions in an attempt to ascertain more details about the system's specifications. A savvy intruder might even get the accounting person to say a username and password. As you can see, this method is based on how well the prospective intruder can manipulate people and actually has little to do with computer skills.

The growing popularity of wireless networks gave rise to new kinds of attacks. One such activity is *war-driving*. This type of attack is an offshoot of *war-dialing*. With war-dialing, a hacker sets up a computer to call phone numbers in sequence until another computer answers to try to gain entry to its system. War-driving is much the same concept, applied to locating vulnerable wireless networks. In this scenario, the hacker simply drives around trying to locate wireless networks. Many people forget that their wireless network signal often extends as much as 100 feet (thus, past walls). At the 2004 DefCon convention for hackers, there was a war-driving contest where contestants drove around the city trying to locate as many vulnerable wireless networks as they could (BlackBeetle, 2004). These sorts of contests are now common at various hacking conventions.

Recent technological innovations have introduced new variations of war driving/dialing. Now we have war flying. The attacker uses a small private drone equipped with Wi-Fi sniffing and cracking software, flies the drone in the area of interest, and attempts to gain access to wireless networks.

Of course, Wi-Fi hacking is only one sort of breach. Password cracking tools are now commonly available on the Internet. We will examine some of these later in this book. There are also exploits of software vulnerabilities that allow one to gain access to the target computer.

DoS Attacks

In a DoS, the attacker does not actually access the system. Rather, this person simply blocks access from legitimate users (CERT, 2003). One common way to prevent legitimate service is to flood the targeted system with so many false connection requests that the system cannot respond to legitimate requests. DoS is a very common attack because it is so easy.

In recent years there has been a proliferation of DoS tools available on the Internet. One of the most common such tools is the Low Orbit Ion Cannon (LOIC). Because these tools can be downloaded for free from the Internet, anyone can execute a DoS attack, even without technical skill.

We also have variations, such as the DDoS attack. This uses multiple machines to attack the target. Given that many modern websites are hosted in network clusters or even in clouds, it is very difficult for a single attacking machine to generate enough traffic to take down a web server. But a network of hundreds or even thousands of computers certainly can. We will explore DoS and DDoS attacks in more detail in Chapter 4, "Denial of Service Attacks."

Web Attacks

By their nature, web servers have to allow communications. Oftentimes, websites allow users to interact with the website. Any part of a website that allows for user interaction is also a potential point for attempting a web-based attack. SQL injections involve entering SQL (Structured Query Language) commands into login forms (username and password text fields) in an attempt to trick the server into executing those commands. The most common purpose is to force the server to log the attacker on, even though the attacker does not have a legitimate username and password. While SQL injection is just one type of web attack, it is the most common.

SQL Injection

SQL injection is still quite common, though it has been known for many years. Unfortunately, not enough web developers take the appropriate steps to remediate the vulnerabilities that make this attack possible. Given the prevalence of this attack, it warrants a bit more detailed description.

Consider one of the simplest forms of SQL injection, used to bypass login screens. The website was developed in some web programming language, such as PHP or ASP.NET. The database is most likely a basic relational database such as Oracle, SQL Server, MySQL, or PostGres. SQL is used to communicate with the database, so we need to put SQL statements into the web page that was written into some programming language. That will allow us to query the database and see if the username and password are valid.

SQL is relatively easy to understand; in fact, it looks a lot like English. There are commands like `SELECT` to get data, `INSERT` to put data in, and `UPDATE` to change data. In order to log in to a website, the web page has to query a database table to see if that username and password are correct. The general structure of SQL is like this:

```
select column1, column2 from tablename
```

or

```
select * from tablename;
Conditions:
select columns from tablename where condition;
```

For example:

```
SELECT * FROM tblUsers WHERE USERNAME = 'jsmith'
```

This statement retrieves all the columns or fields from a table named `tblUsers` where the username is `jsmith`.

The problem arises when we try to put SQL statements into our web page. Recall that the web page was written in some web language such as PHP or ASP.net. If you just place SQL statements directly in the web page code, an error will be generated. The SQL statements in the programming code for the website have to use quotation marks to separate the SQL code from the programming code. A typical SQL statement might look something like this:

```
"SELECT * FROM tblUsers WHERE USERNAME = '" + txtUsername.Text +' AND PASSWORD = '" +
txtPassword.Text +"'" .
```

If you enter username `'jdoe'` and the password `'password'`, this code produces this SQL command:

```
SELECT * FROM tblUsers WHERE USERNAME = 'jdoe' AND PASSWORD = 'password'
```

This is fairly easy to understand even for nonprogrammers. And it is effective. If there is a match in the database, that means the username and password match. If no records are returned from the database, that means there was no match, and this is not a valid login.

The most basic form of SQL injection seeks to subvert this process. The idea is to create a statement that will always be true. For example, instead of putting an actual username and password into the appropriate text fields, the attacker will enter `'` or `'1' = '1` into the username and password boxes. This will cause the program to create this query:

```
SELECT * FROM tblUsers WHERE USERNAME = '' or '1' = '1' AND PASSWORD = '' or '1' = '1'.
```

So you are telling the database and application to return all records where username and password are blank or if 1 = 1. It is highly unlikely that the username and password are blank. But I am certain that 1 =1 always. Any true statement can be substituted. Examples are a = a and bob = bob.

The tragedy of this attack is that it is so easy to prevent. If the web programmer would simply filter all input prior to processing it, then this type of SQL injection would be impossible. That means that before any user input is processed, the web page programming code looks through that code for common SQL injection symbols, scripting symbols, and similar items. It is true that each year fewer and fewer websites are susceptible to this. However, while writing this chapter there was a report that the Joomla Content Management System, used by many web developers, was susceptible to SQL injection.[3]

Cross-Site Scripting

This attack is closely related to SQL injection. It involves entering data other than what was intended, and it depends on the web programmer not filtering input. The perpetrator finds some area of a website that allows users to type in text that other users will see and then instead injects client-side script into those fields.

[3] https://blog.perimeterx.com/joomla-cve-2015-7297/

Note

Before I describe this particular crime, I would point out that the major online retailers such as eBay and Amazon.com are not susceptible to this attack; they do filter user input.

To better understand this process, let's look at a hypothetical scenario. Let's assume that ABC online book sales has a website. In addition to shopping, users can have accounts with credit cards stored, post reviews, and more. The attacker first sets up an alternate web page that looks as close to the real one as possible. Then the attacker goes to the real ABC online book sales website and finds a rather popular book. He goes to the review section, but instead of typing in a review he types in this:

```
<script> window.location = "http://www.fakesite.com"; </script>
```

Now when users go to that book, this script will redirect them to the fake site, which looks a great deal like the real one. The attacker then can have the website tell the user that his session has timed out and to please log in again. That would allow the attacker to gather a lot of accounts and passwords. That is only one scenario, but it illustrates the attack.

Session Hijacking

Session hijacking can be rather complex to perform. For that reason, it is not a very common form of attack. Simply put, the attacker monitors an authenticated session between the client machine and the server and takes that session over. We will explore specific methods of how this is done later in this book.

A 1985 paper written by Robert T. Morris titled "A Weakness in the 4.2BSD Unix TCP/IP Software" defined the original session hijacking.

By predicting the initial sequence number, Morris was able to spoof the identity of a trusted client to a server. This is much harder to do today.

In addition to flags (syn, ack, syn-ack), the packet header will contain the sequence number that is intended to be used by the client to reconstitute the data sent over the stream in the correct order. If you are unfamiliar with network packet flags, we will be exploring that topic in Chapter 2, "Networks and the Internet."

The Morris attack and several other session hijacking attacks require the attacker to be connected to the network and to simultaneously knock the legitimate user offline and then pretend to be that user. As you can probably imagine, it is a complex attack.

Insider Threats

Insider threats are a type of security breach. However, they present such a significant issue that we will deal with them separately. An insider threat is simply when someone inside your organization either misuses his access to data or accesses data he is not authorized to access.

The most obvious case is that of Edward Snowden. For our purposes we can ignore the political issues connected with his case and instead focus solely on the issue of insiders accessing information and using it in a way other than what was authorized.

In 2009 Edward Snowden was working as a contractor for Dell, which manages computer systems for several U.S. government agencies. In March 2012 he was assigned to an NSA location in Hawaii. While there he convinced several people at that location to provide him with their login and password, under the pretense of performing network administrative duties. Some sources dispute whether or not this is the specific method he used, but it is the one most widely reported. Whatever method he used, he accessed and downloaded thousands of documents that he was not authorized to access.

Again, ignoring the political issues and the content of the documents, our focus is on the security issues. Clearly there were inadequate security controls in place to detect Edward Snowden's activities and to prevent him from disclosing confidential documents. While your organization may not have the high profile that the NSA has, any organization is susceptible to insider threats. Theft of trade secrets by insiders is a common business concern and has been the focus of many lawsuits against former employees. In both Chapter 7, "Industrial Espionage in Cyberspace," and Chapter 9, "Computer Security Technology," we will see some countermeasures to mitigate this threat.

While Edward Snowden is an obvious example of insider threats, that is only one example. A common scenario is when someone who has legitimate access to some particular source of data chooses either to access data he is not authorized to access or to use the data in a manner other than how he has been authorized. Here are a few examples:

- A hospital employee who accesses patient records to use the data to steal a patient's identity, or someone with no access at all who accesses records.
- A salesperson who takes the list of contacts with him before leaving the company.

This is actually a much greater problem than many people appreciate. Within an organization, information security is often more lax than it should be. Most people are more concerned with external security than internal security, so it is often rather easy to access data within an organization. In my career as a security consultant, I have seen networks where sensitive data is simply placed on a shared drive with no limiting of access to it. That means anyone on the network can access that data. In a case such as this, no crime has been committed. However, in other cases, employees purposefully circumvent security measures to access data they are not authorized to. The most common method is to simply log in with someone else's password. That enables the perpetrator to access whatever resources and data to which that other person has been granted access. Unfortunately, many people use weak passwords or, worse, they write their password somewhere on their desk. Some users even share passwords. For example, suppose a sales manager is out sick but wants to check to see if a client has emailed her. So she calls her assistant and gives him her login so he can check her email. This sort of behavior should be strictly prohibited by company security policies, but it still occurs. The problem is that now two people have the sales manager's login. Either one could use it or reveal it to someone else (accidentally or on purpose). So there is a greater chance of someone using that manager's login to access data he has not been authorized to access.

DNS Poisoning

Most of your communication on the Internet will involve DNS, or Domain Name Service. DNS is what translates the domain names you and I understand (like www.ChuckEasttom.com) into IP addresses that computers and routers understand. DNS poisoning uses one of several techniques to compromise that process and redirect traffic to an illicit site, often for the purpose of stealing personal information.

Here is one scenario whereby an attacker might execute a DNS poisoning attack:

First the attacker creates a phishing website. It spoofs a bank that we will call ABC Bank. The attacker wants to lure users there so he can steal their passwords and use those on the real bank website. Since many users are too smart to click on links, he will use DNS poisoning to trick them.

The attacker creates his own DNS server. (Actually, this part is relatively easy.) Then he puts two records in that DNS server. The first is for the ABC Bank website, pointing to his fake site rather than the real bank site. The second entry is for a domain that does not exist. The attacker can search domain registries until he finds one that does not exist. For illustration purposes, we will refer to this as XYZ domain.

Then the attacker sends a request to a DNS server on the target network. That request purports to be from any IP address within the target network and is requesting the DNS server resolve the XYZ domain.

Obviously the DNS server does not have an entry for the XYZ domain since it does not exist. So it begins to propagate the request up its chain of command eventually to its service provider DNS server. At any point in that process the attacker sends a flood of spoofed responses claiming to be from a DNS server that the target server is trying to request records from but are actually coming from his DNS server and offering the IP address for XYZ domain. At that point the hacker's DNS server offers to do a zone transfer, exchanging all information with the target server. That information includes the spoofed address for ABC Bank. Now the target DNS server has an entry for ABC Bank that points to the hacker's website rather than the real ABC Bank website. Should users on that network type in the URL for ABC Bank, their own DNS server will direct them to the hacker's site.

This attack, like so many, depends on vulnerabilities in the target system. A properly configured DNS server should never perform a zone transfer with any DNS server that is not already authenticated in the domain. However, the unfortunate fact is that there are plenty of DNS servers that are not properly configured.

New Attacks

Many of the threats discussed in the first two editions of this book are still plaguing network security. Malware, DoS, and other such attacks are just as common today as they were 5 years ago or even 10 years ago.

One new phenomenon is doxing, which is the process of finding personal information about an individual and broadcasting it, often via the Internet. This can be any personal information about any person. However, it is most often used against public figures. While writing this book, the director of the CIA was the target of doxing.[4]

[4] http://gawker.com/wikileaks-just-doxxed-the-head-of-the-cia-1737871619

Hacking of medical devices is also a new attack. Hacker Barnaby Jack first revealed a vulnerability in an insulin pump that could allow an attacker to take control of the pump and cause it to dispense the entire reservoir of insulin in a single does, thus killing the patient.[5] To date there are no confirmed incidents of this having actually been done, but it is disturbing nonetheless. Similar security flaws have been found in pacemakers.

In July 2015 it was revealed that Jeep vehicles could be hacked and shut down during normal operation.[6] This means that a hacker could cause the Jeep to stop in the middle of heavy, high-speed traffic. This has the potential to cause a serious automobile accident.

All of these attacks show a common theme. As our lives become more interconnected with technology, there are new vulnerabilities. Some of these vulnerabilities are not merely endangering data and computer systems, but potentially endangering lives.

Assessing the Likelihood of an Attack on Your Network

How likely are these attacks? What are the real dangers facing you as an individual or your organization? What are the most likely attacks, and what are your vulnerabilities? Let's take a look at what threats are out there and which ones are the most likely to cause you or your organization problems.

At one time, the most likely threat to individuals and large organizations was the computer virus. And it is still true that in any given month, several new virus outbreaks will be documented. This situation means that new viruses are being created all the time and old ones are still out there. However, there are other very common attacks, such as spyware. Spyware is fast becoming as big a problem, even bigger than viruses.

After viruses, the most common attack is unauthorized usage of computer systems. Unauthorized usage includes everything from DoS attacks to outright intrusion of your system. It also includes internal employees misusing system resources. The first edition of this book referenced a survey by the Computer Security Institute of 223 computer professionals showing over $445 million in losses due to computer security breaches. In 75% of the cases, an Internet connection was the point of attack, while 33% of the professionals cited the location as their internal systems. A rather astonishing 78% of those surveyed detected employee abuse of systems/Internet (Computer Security Institute, 2002). This statistic means that in any organization, one of the chief dangers might be its own employees. A 2007 study by Jeffery Johnson and Zolt Ugray, of Utah State University, showed similar problems. And in 2015/2016 similar threats still exist with only slight changes in the percentages.

The 2014 Data Breach Investigation Report from Verizon surveyed 63,437 security incidents with 1,367 confirmed breaches in 95 countries. This survey still showed significant employee abuse of the

[5] http://go.bloomberg.com/tech-blog/2012-02-29-hacker-shows-off-lethal-attack-by-controlling-wireless-medical-device/

[6] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

network as well as many of the familiar attacks we have already discussed in this chapter. The 2015 Data Breach Investigation Report did not show significant improvement.

Basic Security Terminology

Before you embark on the rest of this chapter and this book, it is important to know some basic terminology. The security and hacking terms in this section are merely an introduction to computer security terminology, but they are an excellent starting point to help you prepare for learning more about computer security. Additional terms will be introduced throughout the text and listed in the Glossary at the end of this book.

The world of computer security takes its vocabulary from both the professional security community and the hacker community.

Hacker Slang

You probably have heard the term *hacker* used in movies and in news broadcasts. Most people use it to describe any person who breaks into a computer system. In the hacking community, however, a hacker is an expert on a particular system or systems, a person who simply wants to learn more about the system. Hackers feel that looking at a system's flaws is the best way to learn about that system. For example, someone well versed in the Linux operating system who works to understand that system by learning its weaknesses and flaws would be a hacker.

This process does often mean seeing if a flaw can be exploited to gain access to a system. This "exploiting" part of the process is where hackers differentiate themselves into three groups:

- A white hat hacker, upon finding some flaw in a system, will report the flaw to the vendor of that system. For example, if a white hat hacker were to discover some flaw in Red Hat Linux, he would then email the Red Hat company (probably anonymously) and explain exactly what the flaw is and how it was exploited. White hat hackers are often hired specifically by companies to do penetration tests. The EC Council even has a certification test for white hat hackers: the Certified Ethical Hacker test.
- A black hat hacker is the person normally depicted in the media. Once she gains access to a system, her goal is to cause some type of harm. She might steal data, erase files, or deface websites. Black hat hackers are sometimes referred to as crackers.
- A gray hat hacker is normally a law-abiding citizen, but in some cases will venture into illegal activities.

Regardless of how hackers view themselves, intruding on any system is illegal. This means that technically speaking all hackers, regardless of the color of the metaphorical hat they may wear, are in violation of the law. However, many people feel that white hat hackers actually perform a service by finding flaws and informing vendors before those flaws are exploited by less ethically inclined individuals.

Script Kiddies

A hacker is an expert in a given system. As with any profession, it includes its share of frauds. So what is the term for someone who calls himself a hacker but lacks the expertise? The most common term for this sort of person is *script kiddy* (Raymond, 1993). Yes, that is an older resource, but the term still means the same thing. The name comes from the fact that the Internet is full of utilities and scripts that one can download to perform some hacking tasks. Many of these tools have an easy-to-use graphical user interface that allows someone with very little if any skill to operate the tool. A classic example is the Low Earth Orbit Ion Cannon tool for executing a DoS attack. Someone who downloads such a tool without really understanding the target system is considered a script kiddy. A significant number of the people you are likely to encounter who call themselves hackers are, in reality, mere script kiddies.

Ethical Hacking: Penetration Testers

When and why would someone give permission to another party to hack his system? The most common answer is in order to assess system vulnerabilities. This used to be called a *sneaker*, but now the term *penetration tester* is far more widely used. Whatever the term, the person legally breaks into a system in order to assess security deficiencies, such as portrayed in the 1992 film *Sneakers*, starring Robert Redford, Dan Aykroyd, and Sidney Poitier. More and more companies are soliciting the services of such individuals or firms to assess their vulnerabilities.

Anyone hired to assess the vulnerabilities of a system should be both technically proficient and ethical. Run a criminal background check, and avoid those people with problem pasts. There are plenty of legitimate security professionals available who know and understand hacker skills but have never committed security crimes. If you take the argument that hiring convicted hackers means hiring talented people to its logical conclusion, you could surmise that obviously those in question are not as good at hacking as they would like to think because they were caught.

Most importantly, giving a person with a criminal background access to your systems is on par with hiring a person with multiple DWI convictions to be your driver. In both cases, you are inviting problems and perhaps assuming significant civil liabilities.

Also, some review of their qualifications is clearly in order. Just as there are people who claim to be highly skilled hackers yet are not, there are those who will claim to be skilled penetration testers yet lack the skills truly needed. You would not want to inadvertently hire a script kiddy who thinks she is a penetration tester. Such a person might then pronounce your system quite sound when, in fact, it was simply a lack of skills that prevented the script kiddy from successfully breaching your security. Later in this book, in Chapter 11, "Network Scanning and Vulnerability Scanning," we discuss the basics of assessing a target system. In Chapter 11 we also discuss the qualifications you should seek in any consultant you might hire for this purpose.

Phreaking

One specialty type of hacking involves breaking into telephone systems. This subspecialty of hacking is referred to as *phreaking*. The *New Hacker's Dictionary* actually defines phreaking as "the action of using mischievous and mostly illegal ways in order to not pay for some sort of telecommunications bill, order, transfer, or other service" (Raymond, 2003). Phreaking requires a rather significant knowledge of telecommunications, and many phreakers have some professional experience working for a phone company or other telecommunications business. Often this type of activity is dependent upon specific technology required to compromise phone systems more than simply knowing certain techniques.

Professional Terms

Most hacker terminology, as you may have noticed, is concerned with the activity (phreaking) or the person performing the activity (penetration tester). In contrast, security professional terminology describes defensive barrier devices, procedures, and policies. This is quite logical because hacking is an offensive activity centered on attackers and attack methodologies, whereas security is a defensive activity concerning itself with defensive barriers and procedures.

Security Devices

The most basic security device is the *firewall*. A firewall is a barrier between a network and the outside world. Sometimes a firewall takes the form of a standalone server, sometimes a router, and sometimes software running on a machine. Whatever its physical form, a firewall filters traffic entering and exiting the network. A *proxy server* is often used with a firewall to hide the internal network's IP address and present a single IP address (its own) to the outside world.

Firewalls and proxy servers guard the perimeter by analyzing traffic (at least inbound and in many cases outbound as well) and blocking traffic that has been disallowed by the administrator. These two safeguards are often augmented by an *intrusion detection system* (IDS). An IDS simply monitors traffic, looking for suspicious activity that might indicate an attempted intrusion. We will examine these technologies, and others, in Chapter 9.

Security Activities

In addition to devices, we have activities. *Authentication* is the most basic security activity. It is merely the process of determining if the credentials given by a user or another system (such as a username and password) are authorized to access the network resource in question. When you log in with your username and password, the system will attempt to authenticate that username and password. If it is authenticated, you will be granted access.

Another crucial safeguard is *auditing*, which is the process of reviewing logs, records, and procedures to determine if these items meet standards. This activity will be mentioned in many places throughout this book and will be a definite focus in a few chapters.

The security and hacking terms that we have just covered are only an introduction to computer security terminology, but they provide an excellent starting point that will help you prepare for learning more about computer security. Additional terms will be introduced throughout the text as needed and compiled in the Glossary at the end of the book.

Concepts and Approaches

The approach you take toward security influences all subsequent security decisions and sets the tone for the entire organization's network security infrastructure. Before we delve into various network security paradigms, let us take a moment to examine a few concepts that should permeate your entire thinking about security.

The first concept is the *CIA triangle*. This does not refer to clandestine operating involving the Central Intelligence Agency; rather, it is a reference to the three pillars of security: confidentiality, integrity, and availability. When you are thinking about security, your thought processes should always be guided by these three principles. First and foremost, are you keeping the data confidential? Does your approach help guarantee the integrity of data? And does your approach still make the data readily available to authorized users?

Another important concept to keep in mind is *least privileges*. This means that each user or service running on your network should have the least number of privileges/access required to do her job. No one should be granted access to anything unless it is absolutely required for the job. In military and intelligence circles this is referred to as "need to know."

Network security paradigms can be classified by either the scope of security measures taken (perimeter, layered) or how proactive the system is.

In a *perimeter security approach*, the bulk of security efforts are focused on the perimeter of the network. This focus might include firewalls, proxy servers, password policies, or any technology or procedure to make unauthorized access of the network less likely. Little or no effort is put into securing the systems within the network. In this approach the perimeter is secured, but the various systems within that perimeter are often vulnerable.

There are additional issues regarding perimeter security that include physical security. That can include fences, closed-circuit TV, guards, locks, and so on, depending on the security needs of your organization.

The perimeter approach is clearly flawed, so why do some companies use it? Small organizations might use the perimeter approach if they have budget constraints or inexperienced network administrators. A perimeter method might be adequate for small organizations that do not store sensitive data, but it rarely works in a larger corporate setting.

A *layered security approach* is one in which not only is the perimeter secured, but individual systems within the network are also secured. All servers, workstations, routers, and hubs within the network are secure. One way to accomplish this is to divide the network into segments and secure each segment as if it were a separate network, so if the perimeter security is compromised, not all the internal systems are affected. This is the preferred method whenever possible.

You should also measure your security approach by how proactive/reactive it is. This is done by gauging how much of the system's security infrastructure and policies are dedicated to preventive measures and how much of the security system is designed to respond to attack. A passive security approach takes few or no steps to prevent an attack. A dynamic or proactive defense is one in which steps are taken to prevent attacks before they occur.

One example of this defense is the use of IDSs, which work to detect attempts to circumvent security measures. These systems can tell a system administrator that an attempt to breach security has been made, even if that attempt is not successful. IDSs can also be used to detect various techniques intruders use to assess a target system, thus alerting a network administrator to the potential for an attempted breach before the attempt is even initiated.

In the real world, network security is usually not completely in one paradigm or another; it is usually a hybrid approach. Networks generally include elements of both security paradigms. The two categories also combine. One can have a network that is predominantly passive but layered, or one that is primarily perimeter but proactive. It can be helpful to consider approaches to computer security along a Cartesian coordinate system, as illustrated in Figure 1.1, with the *x* axis representing the level of passive-active approaches and the *y* axis depicting the range from perimeter to layered defense.

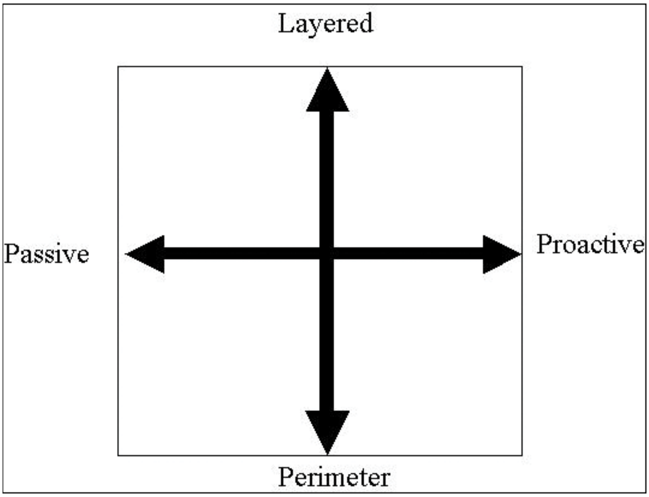

FIGURE 1.1 The security approach guide.

The most desirable hybrid approach is a layered paradigm that is dynamic, which is the upper-right quadrant of the figure.

How Do Legal Issues Impact Network Security?

An increasing number of legal issues affect how one approaches computer security. If your organization is a publicly traded company, a government agency, or does business with either one, there may be legal constraints regarding your network security. Even if your network is not legally bound to these security guidelines, it's useful to understand the various laws impacting computer security. You may choose to apply them to your own security standards.

One of the oldest pieces of legislation in the United States that affects computer security is the Computer Security Act of 1987 (100th Congress, 1987). It requires government agencies to identify sensitive systems, conduct computer security training, and develop computer security plans. This law was a vague mandate ordering federal agencies in the United States to establish security measures, but it did not specify standards.

This legislation established a legal mandate to enact specific standards, paving the way for future guidelines and regulations. It also helped define terms, such as what information is considered "sensitive." This quote is found in the legislation itself:

> The term 'sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (100th Congress, 1987)

This definition of the word *sensitive* should be kept in mind because it is not just social security information or medical history that must be secured.

When considering what information needs to be secure, simply ask this question: Would the unauthorized access or modification of this information adversely affect your organization? If the answer is yes, then you must consider that information sensitive and in need of security precautions.

Another more specific federal law that applied to mandated security for government systems was OMB Circular A-130 (specifically, Appendix III). This document required that federal agencies establish security programs containing specified elements. It also described requirements for developing standards for computer systems and for records held by government agencies.

Most states have specific laws regarding computer security, such as legislation like the Computer Crimes Act of Florida, the Computer Crime Act of Alabama, and the Computer Crimes Act of Oklahoma. If you're responsible for network security, you might find yourself part of a criminal investigation. This could be an investigation into a hacking incident or employee misuse of computer resources. A list of computer crime laws (organized by state) can be found at http://criminal.findlaw.com/criminal-charges/cyber-crimes.html.

Caution

Privacy Laws

It is critical to keep in mind that any law that governs privacy (such as the Health Insurance Portability and Accountability Act of 1996, HIPAA) also has a direct impact on computer security. If your system is compromised, and thus data that is covered under any privacy statute is compromised, you may need to prove that you exercised due diligence in protecting that data. If it can be shown that you did not take proper precautions, you might be found civilly liable.

Online Security Resources

As you read this book, and when you move out into the professional world, you will have frequent need for additional security resources. Appendix B, “Resources,” includes a more complete list of resources, but this section highlights a few of the most important ones you may find useful now.

CERT

The *Computer Emergency Response Team* (CERT, www.cert.org) is sponsored by Carnegie-Mellon University. CERT was the first computer incident-response team, and it is still one of the most respected in the industry. Anyone interested in network security should visit the site routinely. On the website you will find a wealth of documentation, including guidelines for security policies, cutting-edge security research, and more.

Microsoft Security Advisor

Because so many computers today run Microsoft operating systems, another good resource is the Microsoft Security Advisor website: https://technet.microsoft.com/en-us/library/security/dn631936.aspx. This site is a portal to all Microsoft security information, tools, and updates. If you use any Microsoft software, then it is advised that you visit this website regularly.

F-Secure

The F-Secure corporation maintains a website at www.f-secure.com. This site is, among other things, a repository for detailed information on virus outbreaks. Here you will find not only notifications about a particular virus but detailed information about the virus. This information includes how the virus spreads, ways to recognize the virus, and frequently, specific tools for cleaning an infected system of a particular virus.

SANS Institute

The SANS Institute website (www.sans.org) is a vast repository of security-related documentation. On this site you will find detailed documentation on virtually every aspect of computer security you can imagine. The SANS Institute also sponsors a number of security research projects and publishes information about those projects on its website.

Summary

Network security is a complex and constantly evolving field. Practitioners must stay on top of new threats and solutions and be proactive in assessing risk and protecting their networks. The first step to understanding network security is to become acquainted with the actual threats posed to a network. Without a realistic idea of what threats might affect your systems, you will be unable to effectively protect them. It is also critical that you acquire a basic understanding of the terminology used by both security professionals and those who would seek to compromise your security.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. One extreme viewpoint about computer security is what?

   A. The federal government will handle security.
   B. Microsoft will handle security.
   C. There are no imminent dangers to your system.
   D. There is no danger if you use Linux.

2. Before you can formulate a defense for a network you need what?

   A. Appropriate security certifications
   B. A clear picture of the dangers to be defended against
   C. To finish this textbook
   D. The help of an outside consultant

3. Which of the following is not one of the three major classes of threats?

   A. Attempts to intrude on the system
   B. Online auction fraud
   C. Denial of service attacks
   D. A computer virus

4. What is a computer virus?

   A. Any program that is downloaded to your system without your permission
   B. Any program that self-replicates
   C. Any program that causes harm to your system
   D. Any program that can change your Windows Registry

5. What is spyware?

   A. Any software that monitors your system
   B. Only software that logs keystrokes
   C. Any software used to gather intelligence
   D. Only software that monitors what websites you visit

6. What is a penetration tester?

   A. A person who hacks a system without being caught
   B. A person who hacks a system by faking a legitimate password
   C. A person who hacks a system to test its vulnerabilities
   D. A person who is an amateur hacker

7. What is the term for hacking a phone system?

   A. Telco-hacking
   B. Hacking
   C. Cracking
   D. Phreaking

8. What is malware?

   A. Software that has some malicious purpose
   B. Software that is not functioning properly
   C. Software that damages your system
   D. Software that is not properly configured for your system

9. What is war-driving?

   A. Driving and seeking a computer job
   B. Driving while using a wireless connection to hack
   C. Driving looking for wireless networks to hack
   D. Driving and seeking rival hackers

10. When a hacking technique uses persuasion and deception to get a person to provide information to help compromise security, this is referred to as what?

   A. Social engineering
   B. Conning
   C. Human intel
   D. Soft hacking

11. What is the most common threat on the Internet?

    A. Auction fraud
    B. Hackers
    C. Computer viruses
    D. Illegal software

12. What are the three approaches to security?

    A. Perimeter, layered, hybrid
    B. High security, medium security, low security
    C. Internal, external, and hybrid
    D. Perimeter, complete, none

13. An intrusion detection system is an example of which of the following?

    A. Proactive security
    B. Perimeter security
    C. Hybrid security
    D. Good security practices

14. Which of the following is the most basic security activity?

    A. Authentication
    B. Firewalls
    C. Password protection
    D. Auditing

15. The most desirable approach to security is one that is which of the following?

    A. Perimeter and dynamic
    B. Layered and dynamic
    C. Perimeter and static
    D. Layered and static

16. According to a recent survey of 223 computer professionals prepared by the Computer Security Institute, which of the following was cited as an issue by more of the respondents?

    A. Internal systems
    B. Employee abuse
    C. Routers
    D. Internet connection

17. Which of the following types of privacy law affects computer security?
    - A. Any state privacy law
    - B. Any privacy law applicable to your organization
    - C. Any privacy law
    - D. Any federal privacy law

18. The first computer incident-response team is affiliated with what university?
    - A. Massachusetts Institute of Technology
    - B. Carnegie-Mellon University
    - C. Harvard University
    - D. California Technical University

19. Which of the following is the best definition of the term *sensitive information*?
    - A. Any information that has impact on national security
    - B. Any information that is worth more than $1,000
    - C. Any information that if accessed by unauthorized personnel could damage your organization in any way
    - D. Any information that is protected by privacy laws

20. Which of the following is a major resource for detailed information on a computer virus?
    - A. The MIT Virus Library
    - B. The Microsoft Virus Library
    - C. The F-Secure Virus Library
    - D. The National Virus Repository

EXERCISES

EXERCISE 1.1: How Many Virus Attacks Have Occurred This Month?

1. Using some website resource, such as www.f-secure.com, look up recent computer virus outbreaks.

2. How many virus outbreaks have occurred in the past 7 days?

3. Write down how many outbreaks there have been in the past 30 days, 90 days, and 1 year.

4. Are virus attacks increasing in frequency?

EXERCISE 1.2: Learning About Cookies as Spyware

1. Get an idea of what kind of information cookies store. You might find the following websites helpful:

   www.allaboutcookies.org/
   www.howstuffworks.com/cookie1.htm

2. Write a brief essay explaining in what way cookies can invade privacy.

EXERCISE 1.3: Hacker Terminology

1. Use the *Hacker's Dictionary* at http://www.outpost9.com/reference/jargon/jargon_toc.html.

   Hacker terms:

   A. Alpha geek
   B. Grok
   C. Red Book
   D. Wank

EXERCISE 1.4: Using Security Resources

1. Using one of the preferred web resources listed in this chapter, find three policy or procedure documents from that resource.

2. List the documents you selected.

3. Write a brief essay explaining why those particular documents are important to your organization's security.

EXERCISE 1.5: Learning About the Law

1. Using the Web, journals, books, or other resources, find out if your state or territory has any laws specific to computer security. You might find the following websites helpful:

   www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html
   www.cybercrime.gov/

2. List three laws that you find, with a brief description of each. The list can be a simple one, noting the pertinent laws in your region. Describe each one with one or two sentences.